Introduction to Lawful Interception Standards - Marc Anderson - Medium

Marc Anderson ⋮ 8-10 minutes ⋮ 12/12/2020

First of all, what is Lawful Interception? According to the ETSI standards body:

> “As a legally sanctioned official access to private communications, Lawful Interception (LI) is a security process in which a service provider or network operator collects and provides law enforcement officials with intercepted communications of private individuals or organizations”.

All voice calls, sms, mobile internet sessions and other forms of telecommunications pass through a mobile operator’s core networks. Lawful Interception allows a subscribers’ communications to be intercepted based on their identity (e.g. Phone Number). Interception is triggered in these core network nodes (known from LI point of view, as Network Elements) when that target identity is matched with an identity partaking in a communications session.

Typically an Administration / Mediation Device acts as a single point of access to LI in a network for the LEA (Law Enforcement Agency). In this way, the Law Enforcement Agency does not have direct access to the core network nodes in the operators’ network, which is desirable from a security point of view.

Historically the interfaces between the core network nodes and the Administration / Mediation Device have been proprietary. The standard bodies (ETSI & 3GPP) have dealt with the standardizing of the HI (Handover Interface) between the Mediation Device and the LEA. In more recent times, standards have been developed to standardize the interfaces between the Network Elements and the Administration / Mediation Device, and that will be covered in a future article. However, the scope of this article it to explain the Handover Interfaces between the Mediation Device and the Law Enforcement Agency.

There are four handover interfaces that have been defined:

HI1: The transfer of warrant-related notifications from the Administration Device to the Agency

HI2: The transfer of IRI (Intercept Related Information) to the Agency

HI3: The transfer of CC (Contents of Communications) to the Agency.

HI4: The transfer of notifications from the Mediation Device to the Agency.

HI4 is a newly defined, rarely used interface that will not be covered here. Perhaps it will be covered in a future article. This article will focus on the three traditional handover interfaces: HI1, HI2 and HI3.

When a LEA receives permission to intercept a target they generally send the target identity to be intercepted to the CSP (Communications Service Provider, typically a mobile operator). The target identity can be a phone number (MSISDN, TEL URI), SIP URI, IMSI (Sim identifier), IMEI (equipment identifier), etc.

For example, by marking a target with the IMEI it is possible to intercept a subscriber even if they switch sim cards to a different number.

The CSP then provisions this identity to be intercepted. The details needed to intercept a subscriber are described in a warrant. The Law Enforcemenet Agency needs to know when a subscriber is being intercepted. Thus, when a warrant is activated on the network elements, or removed from the network

elements, the Law Enforcement Agency receives a notification over the HI1 interface informing them of this. If activation or termination fails, a HI1 notification would also be sent.

One advantage of this “separation” between Operator and Agency is the extra layer of accountability. Agencies cannot just add new subscribers to be targeted whenever they want. They should follow the process, get a warrant from a judge and when everything is in place, make the request to the mobile operator to add the target to be interceped.

Interception is triggered in a network element when the marked identity is part of a content of communications flowing through that network element. This can be a voice call, an SMS a mobile data session (Bearer, PDP Context, etc), or any other types of communication a network element is handling. When interception is triggered, intercepted data is sent from the network elements to the mediation device which converts the data to the relevant standard and delivers it to the LEA.

There are two types of data delivered during an intercepted communications case: Intercept Related Information (IRI) and Content of Communications (CC).

IRI is metadata about the communications session: the type of communications, the subscribers involved, sometimes the cell id or other location information, etc.

Content of Communications is the intercepted payload: the voice, packet data, etc.

When a warrant is created, a Lawful Intercepted Identifer (LIID) is defined. This uniquely identifies all commmunications associated to that warrant. All IRI and CC packets will include the LIID in their header. Ideally, the LIID should not identify the subscribed being intercepted, so it should not be the target number for example.

All IRI and CC packets belonging to a single communications session (e.g. a voice call) contain a unique correlation identifier so that the LEA can link those together as one call.

All HI records contain the Domain Dd identifying the standard and standard version being used to encode the data.

Most standards allow for a timestamp (either UTC or local time) to be sent with each HI record.

Most standards define a sequence number field, thus it is possible to put the received data in the correct order. This is important as TCP and other delivery protocols do not guarantee packets are received in the same order they were sent. With every HI record that is sent, the sequence number is incremented.

ETSI and 3GPP have traditionally definied similar standards for these interfaces. However, different standards were defined for each technology (Circuit-Switched, Packet-Switced, Evolved-Packet-Switched, IP Multimedia, etc), thus separate decoders needed to be written for each one. Each time a new technology was implemented, a new standard needed to be agreed between the CSP (Communication Service Provider) and the LEA. Each technology had different headers and different fields.

With the advent of the ETSI TS 102 232 delivery standard, a common header can be used across all technologies.

ETSI 232–1 defines the delivery standard, which includes a header and the contents payload. The contents payload can be a subset of one of the traditional standards, or one of the new ones defined by ETSI 232, such as ETSI 232–5 for IPMM or ETSI 232–7 for Packet-Switched Data.

LIID, Communications Identifier, Domain ID and Sequence Number are all mandatory as part of every HI record in ETSI232. Optional parameters often sent include timestamp, interception point id (the node where interception was triggered), and country codes indicating where the warrant was authorized and where the intercepted data was delivered from.

Here are is an example of a decoded HI1 notification sent using ETSI232–1 delivery

pSHeader:
communicationIdentifier:
deliveryCountryCode: US
networkIdentifier:
operatorIdentifier: OPER
lawfulInterceptionIdentifier: ‘12345678’
li-psDomainId: [0, 4, 0, 2, 2, 5, 1, 14]
sequenceNumber: 0
timeStamp: [‘2019’, ‘12’, 08, ‘21’, ‘25’, ‘49’, ‘691’, null]
timeStampQualifier: timeOfMediation
payload:
- hI1-Operation
- — liActivated
— communicationIdentifier:
network-Identifier:
operator-Identifier: OPER
domainID: [0, 4, 0, 2, 2, 0, 1, 6]
lawfulInterceptionIdentifier: ‘12345678’
timeStamp:
— localTime
— generalizedTime: [‘2019’, ‘12’, 08, ‘21’, ‘25’, ‘49’, ‘691’, null]
winterSummerIndication: notProvided

The liActivated event type indicates that this new target with LIID 12345678 has been activated successfully and interception of that subscribers communications will not occur. When the LEA receives this notification, they can match that LIID against their own database and see which subscriber identity this refers to. A similiar event would be sent when the target is terminated and no longer being intercepted.

There are two domains here. 0.4.0.2.5.5.1.14 refers to the ETSI232 standard version: ETSI232 v14. 0.4.0.2.2.0.1.6 refers to the sub-domain of the standard embedded in the payload: ETSI hi1 notificationOperations v6.

For more on ETSI TS 102 232 check out the official standards document, including some nice diagrams:

https://www.etsi.org/deliver/etsi_ts/102200_102299/10223201/03.20.01_60/ts_10223201v032001p.pdf

That’s all for this article. I hope you learned something. More coming soon.